

1 **CLAIMS**

2 1. A method comprising:
3 receiving an event from a first security engine;
4 identifying a second security engine configured to utilize information
5 contained in the event; and
6 communicating the information contained in the event to the second
7 security engine.

8
9 2. A method as recited in claim 1 wherein the event identifies a type of
10 security attack.

11
12 3. A method as recited in claim 1 wherein the event identifies an action
13 performed by the first security engine in response to a security attack.

14
15 4. A method as recited in claim 1 wherein the first security engine and
16 the second security engine are application programs.

17
18 5. A method as recited in claim 1 wherein the first security engine is an
19 antivirus application program.

20
21 6. A method as recited in claim 1 wherein the first security engine is a
22 firewall application program.

1 7. A method as recited in claim 1 wherein the first security engine is an
2 intrusion detection application program.

3
4 8. A method as recited in claim 1 wherein the first security engine is a
5 vulnerability analysis application program.

6
7 9. A method as recited in claim 1 further comprising:
8 identifying a third security engine configured to utilize information
9 contained in the event; and
10 communicating the information contained in the event to the third security
11 engine.

12
13 10. A method as recited in claim 1 further comprising:
14 receiving an updated security policy;
15 identifying at least one security engine associated with the updated security
16 policy; and
17 providing the updated security policy to the identified security engine.

18
19 11. A method as recited in claim 1 further comprising:
20 receiving a request for data from the first security engine; and
21 communicating the requested data to the first security engine.
22
23
24
25

1 **12.** A method as recited in claim 1 further comprising storing
2 information contained in the event in a central location accessible to a plurality of
3 security engines.
4

5 **13.** One or more computer-readable memories containing a computer
6 program that is executable by a processor to perform the method recited in claim
7 1.
8

9 **14.** A method comprising:
10 receiving a security-related event from a first security-related application
11 program;
12 identifying information contained in the security-related event;
13 identifying a second security-related application program associated with
14 the information contained in the security-related event; and
15 communicating the information contained in the security-related event to
16 the second security-related application program.
17

18 **15.** A method as recited in claim 14 wherein the first security-related
19 application program is an antivirus application program.
20

21 **16.** A method as recited in claim 14 wherein the security-related event is
22 associated with system state information.
23
24
25

1 **17.** A method as recited in claim 14 wherein the information contained
2 in the security-related event includes data identifying a type of security attack.

3
4 **18.** A method as recited in claim 14 wherein the information contained
5 in the security-related event includes data identifying an action performed by the
6 first security-related application program in response to a security attack.

7
8 **19.** A method as recited in claim 14 further comprising:
9 receiving system state information from a third security-related application
10 program; and
11 storing the system state information such that the system state information
12 is accessible to the first security-related application program and the second
13 security-related application program.

14
15 **20.** A method as recited in claim 14 further comprising:
16 identifying a third security-related application program associated with the
17 information contained in the security-related event; and
18 communicating the information contained in the security-related event to
19 the third security-related application program.

20
21 **21.** One or more computer-readable memories containing a computer
22 program that is executable by a processor to perform the method recited in claim
23 14.

1 **22.** A system comprising:
2 a first security engine associated with a first type of security attack;
3 a second security engine associated with a second type of security attack;
4 and
5 an event manager coupled to receive events from the first security engine
6 and the second security engine, the event manager further to identify information
7 contained in the events and to identify at least one security engine associated with
8 information contained in a particular event, and further to communicate the
9 information contained in the particular event to the at least one security engine.

10
11 **23.** A system as recited in claim 22 wherein the information contained
12 in the events identifies a type of security attack.

13
14 **24.** A system as recited in claim 22 wherein the information contained
15 in each event identifies an action taken in response to a security attack.

16
17 **25.** A system as recited in claim 22 wherein the information contained
18 in the events includes system state information.

19
20 **26.** A system as recited in claim 22 further comprising a third security
21 engine coupled to the event manager and associated with a third type of security
22 attack.

1 **27.** A system as recited in claim 22 further comprising a storage device
2 coupled to the event manager, the first security engine and the second security
3 engine, the storage device to store event information.

4
5 **28.** One or more computer-readable media having stored thereon a
6 computer program that, when executed by one or more processors, causes the one
7 or more processors to:

8 receive a first security-related event from a first service;
9 identify information contained in the first security-related event;
10 receive a second security-related event from a second service;
11 identify information contained in the second security-related event;
12 communicate information contained in the first security-related event to the
13 second service; and
14 communicate information contained in the second security-related event to
15 the first service.

16
17 **29.** One or more computer-readable media as recited in claim 28
18 wherein the first security-related event identifies a particular type of security
19 attack.

20
21 **30.** One or more computer-readable media as recited in claim 28
22 wherein the one or more processors further store the information contained in the
23 first security-related event and the information contained in the second security-
24 related event for access by other services.

25

1 **31.** One or more computer-readable media as recited in claim 28
2 wherein the one or more processors further communicate information contained in
3 the first security-related event to a third service.
4

5 **32.** One or more computer-readable media as recited in claim 28
6 wherein the first service is associated with a first type of security attack and the
7 second service is associated with a second type of security attack.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25